REPORTING

Computer crime involving state computer resources must be reported to the CHP Computer Crimes Investigation Unit by calling the Emergency Notification and Tactical Alert Center at (916) 657-8287. Be prepared to provide the following information:

- Name, address, and city of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO or system administrator).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating system of the affected computer(s).
- Location of the affected computer(s).
- Type of incident.
- Actions taken after discovery of the incident.

SIMPLE COMPUTER SECURITY TIPS

- **Use strong passwords.** Choose passwords that are difficult or impossible to guess. Passwords should not be recorded and/or affixed to computers, monitors, keyboards, etc. Give different passwords to all accounts.
- **Make regular backups of critical data.** Backups must be made at least once each day. Larger organizations should perform full backup weekly and incremental backups every day. At least once a month the backup media should be verified.
- **Use virus protection software.** Ensure it is on your computer, check daily for new virus signature updates, and scan all the files on your computer periodically.
- **Use a firewall as a gatekeeper between your computer and the Internet.** Firewalls are usually software products. They are essential for those who keep their computers online through broadband connections, such as DSL or cable, but they are also valuable for those who still dial in.
- **Do not keep computers online when not in use.** Either shut them off or physically disconnect them from Internet connection.
- **Do not open e-mail attachments from strangers,** regardless of how enticing the subject line or attachment may be. ***Be suspicious of any unexpected e-mail attachment from someone you do know*** because it may have been sent without that person's knowledge from an infected machine.
- **Regularly download security patches from your software vendors.**

* Consult *www.chp.ca.gov* for more information.

CHP 1040 (rev. 2/06) OPI 040

California Highway Patrol

COMPUTER CRIME REPORTING FOR STATE AGENCIES

LEGAL REQUIREMENTS

Government Code Section 14613.7(a) requires state agencies to report to the California Highway Patrol (CHP) all crimes on state-owned or state-leased property where state employees are discharging their duties. Specifically, Title 13, California Code of Regulations, Division 2, Chapter 12, Section 1875 requires the reporting of computer crimes involving state computer resources. (Note: Notification of a computer crime to a local law enforcement agency or information technology-related investigative task force does not relieve state agencies of their obligation to notify the CHP.)

The CHP has established a Computer Crimes Investigation Unit (CCIU) to investigate any computer-related incidents where state assets and/or personnel are involved. CCIU can be notified of an incident 24 hours a day, seven days a week by calling the Emergency Notification and Tactical Alert Center (ENTAC).

We recommend that representatives of state agencies reporting computer crimes to the CHP follow their established internal departmental notification protocols, including but not limited to, involving the agency's Information Security Officer, or their designee. State agencies reporting computer crimes to ENTAC should be prepared to provide the information identified in the "REPORTING" section of this brochure. When ENTAC receives a report of a computer crime, CCIU investigators are immediately notified.

Depending on the nature of the computer crime reported, a CCIU investigator may respond to, or call, the reporting agency for additional information.

COMPUTER CRIMES THAT REQUIRE IMMEDIATE NOTIFICATION TO THE CHP

The CHP has primary investigative authority for computer-related incidents. The most common violations involve California Penal Code § 502, subsection (c), where a state agency is the victim. Computer crimes occur when a person:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data. (Note: This normally is part of a different crime/ objective, and the computer is only a tool to accomplish the offense.)

(2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network (e.g., a computer user or hacker removing information from the system, when unauthorized to do so).

(3) Knowingly and without permission uses or causes to be used computer services (e.g., someone uses a computer that is not locked to access the Internet or e-mail).

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network (e.g., a computer user or hacker installs unauthorized software).

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network (e.g., someone attacking a website, network, or computer with a zombie or bot computer, thus preventing an authorized user from accessing the services normally provided).

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section (e.g., a computer user giving another user their password to access services not normally accessible by the second user).

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network (e.g., someone other than an authorized user logging in and utilizing the system).

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network (e.g., a computer user or hacker installing any type of virus, worm, or trojan).

(9) Knowingly and without permission uses the Internet domain name of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages, and thereby damages or causes damage to a computer, computer system, or computer network. (Note: Usually found during the process of a phishing scheme or as part of SPAM e-mail.)

Any questions regarding the reporting of computer crimes or any other computer-related incidents can be directed to CCIU. Please call (916) 453-3950, Monday through Friday, 8:00 a.m. to 5:00 p.m., or e-mail at cciu@chp.ca.gov.